# CSC2125 Homework 3

Zi Han Zhao

1001103708

**1 Suppose we run PBFT algorithm on a cluster of 21 machines. What is the maximum number of machines we will be able to tolerant for failure simultaneously?**

We know $N \geqslant 3f+1$ where N is the total number of nodes and f replicas are faulty. Then $21 \geqslant 3f+1$ so $f_{max} = 6$.

**2 A node in PBFT waits for prepare/commit messages from two thirds of nodes (replicas) during the prepare/commit stages. What would happen if the node instead waits for prepare and commit messages from only a simple majority of other nodes? Would the modified PBFT be secure? If not, please explain with a counter example.**

The modified PBFT is not secure anymore. Let's say the number of responses of node A is x where $x < 2f + 1$, $f$ is the number of faulty nodes. Among the x messages, in the worst case, there would be possibly $f$ faulty responses so there are $x - f$ non-faulty responses. It is found that $x - f < f + 1$, which means that non-faulty responses is not greater than faulty responses. Therefore, node A cannot decide the message he received is correct or not.

**3 PBFT relies on the primary node to send out pre-prepare messages to drive the consensus process. What would happen if the primary node is malicious or fails? How does PBFT handle this situation?**